

**A New Taxonomy for Configuration Management:
*Requirements, Technology, and the Design Bases of Nuclear Power
Plants***

B. Williamson^a, W. Merritt^b, J. M. O'Connell^b

^aInterlogic, Inc.

12280 Tower Hill Road
Sawyer, Michigan, USA 49125
bradwmson@interlogic-inc.com

^bStone & Webster Asia, The Shaw Group

600 Technology Center Drive
Stoughton, Massachusetts, USA 02072
wayne.merritt@shawgrp.com
michael.oconnell@shawgrp.com

Abstract: A Configuration Management (CM) taxonomy has been developed that more effectively addresses the management of design bases at both new and existing nuclear production facilities. The proposed taxonomy reflects an emergent understanding of design bases as product requirements that identify critical attributes of the requests and promises inherent in both regulatory and contractual requirements. Consequently, the new taxonomy more completely incorporates the relationships between the physical plant, the design and licensing requirements, and facility documentation. Additionally, and perhaps most importantly, the new taxonomy incorporates a new concept, that of a Design Bases Rule Set, to identify which design related information is required to be maintained within the CM system. This allows the new taxonomy to be cost-effectively used at legacy plants, while allowing new construction to take advantage of the strengths and new possibilities. The new taxonomy is non-source specific, meaning that it can accommodate the regulatory and/or design requirements of any organization or country. It is expected that the new taxonomy would minimize the cost of plant configuration changes and enable the capture of knowledge from an aging and shrinking workforce. Overall, the primary reason for designing a new CM system is the issue of nuclear safety. The foundational approach to CM described here affords a substantially higher degree of confidence in the validity and consistency of the managed CM elements and provides a higher degree of certainty that safety margins are being maintained adequately. This new design for CM will enable a new facility to apply sound CM practices from the initial design phase and manage the relationships between the physical plant, the design and licensing requirements, and facility documentation effectively over the life of the plant.

PRESENTATION:

INTRODUCTION

A Configuration Management taxonomy [1] has been developed that more effectively addresses the management of design bases at both new and existing nuclear production facilities. This taxonomy is the result of efforts of Interlogic, Inc. and Shaw Stone & Webster to design a Configuration Management System (CMS) for implementation in the design and construction of a new nuclear production facility and reflects not only the existing state of the industry but incorporates lessons learned during efforts to design this new CMS.

Having completed the CMS design phase, and making preparations to develop the prototype CMS into a production version for application in the design and construction of several new plants, it has become apparent that the new CMS taxonomy offers substantial power in managing the design bases and associated requirements, improving confidence in the integrity of plant design, and incorporating safety margin management as a standard practice.

The CMS taxonomy has been designed to incorporate all plant design requirements, to be implemented at both new and legacy plants, to allow management of the design bases over the life of the plant, and to address the concerns associated with making changes to the production facility while assuring compliance with regulatory requirements.

Continued operation and development of new nuclear power plants are contingent on two critical attributes, trust and economics. Trust is represented in the confidence that the public has that the technology is safely designed and operated and that it is not a significant hazard. Economics is represented in the cost of operations of this technology as compared to alternatives for energy generation. Both attributes are intertwined in the purpose of a Configuration Management System.

In essence, a Configuration Management System is the means by which the plant owner-operator keeps the promise of safe operation by ensuring that the design can perform as planned over a long period of time. The public comes to trust the facility owner-operator as the promises about safe operation are kept recurrently over time. In contrast, trust is broken when the public discovers, usually through outside inspection, but sometimes revealed by plant transients and accidents, that the operation of a nuclear unit is not as safe as promised.

Notice we are not talking about engineering margin or probabilistic risk assessment figures: the public does not know what those numbers mean, but the public does know when promises are kept or broken. The betrayal of the public trust has significant impact on the economics of operation. Knowing that, what is the role of the new taxonomy for Configuration Management in managing trust and supporting economic operations?

HISTORY OF THE DESIGN BASES TAXONOMY

The original design and construction of most operating nuclear production facilities today predates the discipline of configuration management. Consequently, these facilities found themselves, at some point in their history, without adequate mechanisms to ensure reasonable correlation between regulatory requirements, facility documentation, and the physical configuration of the facility itself. Consequently, many facilities were unable to maintain a reasonable level of trust with the public in their geographic area.

In the United States (US), many plants experienced this dilemma when confronted with the task of replacing components that had failed and discovering that the original vendors were no longer in existence, or no longer manufactured a suitable 'like-for-like' replacement. In the course of identifying the original design requirements for these components, it quickly became apparent that a mechanism was needed to connect plant structures, systems, and components (SSCs) to the original design requirements. Since this mechanism had not been incorporated within the original design and construction of the facilities, there was no clear methodology for the reconstitution of what we now call the 'design bases'.

A variety of methodologies and mechanisms were used to reconstitute design bases with varying degrees of success. One critical limiting factor that quickly emerged was the recognition that reconstitution of the design bases for an operating facility could be prohibitively expensive. This factor alone would be significant enough to specify the scope of design bases recovery efforts and contributed substantially to the permanent closure of one US facility prior to commercial operation but after loading fuel. [2]

Attempts were made to bring clarity and efficiency to the design bases management effort. Through the United States Nuclear Regulatory Commission (USNRC), and the Nuclear Energy Institute (NEI), documentation and guidance were provided in what ultimately became NEI 97-04, "*Guidance and Examples for Identifying 10 CFR 50.2 Design Bases*". This document, as well as others developed through efforts by the Institute of Nuclear Power Operations [3] (INPO) and the International Atomic Energy Agency [4] (IAEA) provided an effective basis for implementing configuration management and back-fitting design bases management to existing plants.

In the last few years, however, we have been faced with a different type of design bases problem; that of designing and implementing a configuration management system during the design and construction of a new nuclear production facility. In the course of our work, we have discovered that existing CMS guidance documents including NEI 97-04, INPO AP-929, and TECDOC 1335 do not address the full range of configuration management concerns predominant in new construction.

The critical problem is two-fold. First, existing methodologies do not provide a mechanism for requirements to flow through documentation into design and actual plant configuration. Secondly, it is confusing and confounding to fail to manage non-regulatory requirements with the same rigor we use to manage regulatory requirements.

EVOLUTION OF THE CONFIGURATION MANAGEMENT TAXONOMY

Over the two years that it has taken to develop the prototype CMS, the proposed Configuration Management Taxonomy has evolved as we encountered obstacles to a successful implementation.

We recognized that the design requirements necessary for the design, construction, operation, and engineering of new facilities are not limited to regulatory requirements only. The successful implementation of a new nuclear production facility must necessarily address requirements from a variety of sources beyond the regulatory requirements. Our concern for a complete taxonomy of Configuration Management led to the examination of current requirements management efforts at the National Aeronautic and Space Administration (NASA), the Food and Drug Administration (FDA), and Boeing.

We discovered quite sophisticated requirements management practices that incorporate requirements regardless of source, and with tracking mechanisms that provide for revision control of both requirements and physical configurations. These technologies allow for requirement compliance to be demonstrated in computer software, with reporting mechanisms that substantially ease the cost and labor requirements associated with traditional Configuration Management documentation.

These practices and methodologies were evaluated against fundamental strategies for producing action in language such as the request/promise cycle and conversations for action proposed by Winograd and Flores. [5] The result was a taxonomy that would reflect an effective structure of the requirements necessary to design, construct, and operate a nuclear production facility that would effectively connect each structure, system, and component in the physical facility to the requirements that specified its need.

Finally, we recognized that while full implementation of the new CM taxonomy was appropriate and necessary for new construction, the concern over implementation cost could prohibit its adoption at legacy plants. Consequently, we designed a proprietary Design Bases Rule Set that allows the end user to determine systematically what requirements will be incorporated into a limited Configuration Management System.

FEATURES OF NEW CONFIGURATION MANAGEMENT TAXONOMY

What does the new Configuration Management taxonomy do?

Like the Configuration Management methodologies it has evolved from, it provides a methodology for the management of design requirements, plant documentation, and plant configuration.

In contrast to the historical practices, the new CM taxonomy clearly defines the hierarchy of requirements, and through the Design Bases Rule Sets, eliminates confusion regarding the scope of Configuration Management. The days of confusion over the question, "Is this in the Design Bases?" are over!

Using current technology, it enables the management of complex component-to-design-requirement relationships. Unlike the historical systems, engineers will be able to determine

relevant requirements by the simple act of selecting a structure, system, or component in the CMS.

It manages both regulatory and non-regulatory requirements. The new CMS can be used not only for validating regulatory compliance, but also compliance with codes, standards, contracts, and owner design objectives.

Unlike previous methodologies, it incorporates the concept of Design Parameters, which are the critical numbers for plant design and operation, which makes Margin Management and Setpoint Management substantially easier and more intuitive.

Finally, through the use of carefully designed Design Bases Rules Sets, the new CM taxonomy is applicable to both new and existing nuclear production facilities.

NEW CONFIGURATION MANAGEMENT TAXONOMY OVERVIEW

The new Configuration Management taxonomy has been designed to provide a hierarchical connection between requirements and individual structures, systems, and components. To do so, it was necessary to make significant changes to the existing taxonomy. Refer to the new Configuration Management Taxonomy in Figure 1 for the remainder of this discussion.

The Design Bases Rule (DBR) Set specifies which specific requirement sources will be included in the CMS. They can be as precise or as general as desired, ultimately affecting only the scope of material included in the CMS.

It was determined necessary to treat all requirements uniformly. While the CMS will keep track of which requirements are regulatory versus those that are not, the requirement hierarchy does not specify a difference. As a result, concepts such as Design Bases Values and Controlling Parameters (and the associated confusion) are eliminated.

Fig. 1 – New Configuration Management Taxonomy

Requirements are captured verbatim within the CMS regardless of source and parsed (i.e., broken down into smaller parts) as necessary to produce manageable Design Bases Specifications. Software technology makes management of large numbers of complex

B. Williamson et al.

requirements feasible, and opens up the possibility that in the future, if requirement sources adopt common technology for transfer of data, the CMS would read requirements directly from the regulator and other sources.

Design Bases Specifications (DBS) translate the parsed requirements into high level statements that describe how the specific nuclear production facility will implement the requirement. SSC Specifications (SSCS) translate plant-specific DBSs into statements that specify how individual structures, systems, and components will implement the DBSs.

From SSCSs, we move into the historical engineering work. SSCSs generate three classes of information: Supporting Design Information, Design Parameters, and Supporting Operating Information. Supporting Design Information (SDI) is the documents that design and procure individual components, including calculations, drawings, purchase specifications, and orders. Design Parameters (DP) are the values that define characteristics, setpoints, and limits associated with facility structures, systems, and components. Finally, Supporting Operating Information (SOI) is the procedures and documentation necessary to fulfill specific requirements.

Note the change that has been made to connect SSCSs to the documentation, rather than the structure, system, or component (SSC) itself. After all, it is the documentation that specifies the SSC, not the other way around. Finally, at the bottom of the hierarchy, each SSC in the physical facility is represented and connected to the requirements that specify the SSC.

Detailed descriptions of the various components of the new Configuration Management Taxonomy follow.

DESIGN BASES RULE SET

The Design Bases Rule Set ultimately determines which requirements must be managed within the CMS. While the details of the DBRs are proprietary, each DBR is crafted to include and exclude specific requirements within the CMS. Since DBRs determine what design requirements must be managed within the CMS, they determine the scope of the managed information, and consequently the cost of back-fitting the CMS to legacy plants.

Definition: A Design Bases Rule is a statement that specifies or bounds a group of requirements that will be included within the CMS.

Example: Requirements included within Title 10, United States Code of Federal Regulations, Part 50, Appendix A.

Each requirement included in the CMS must reference an associated DBR to justify its inclusion.

DESIGN REQUIREMENTS

Design Requirements include ALL requirements that must be met for the construction and operation of the nuclear production facility as specified by the Design Bases Rule Set. These may include all national and state regulatory requirements, other legal requirements, codes and standards, economic and non-regulatory requirements, and contractual obligations.

B. Williamson et al.

Definition: *A Design Requirement is any statement that specifies capability, capacity, limitations, inclusion, or exclusions **that will be complied with** at a nuclear production facility as determined by an associated Design Bases Rule.*

Example: *10CFR50, App. A, Criterion 34 -- Residual heat removal. A system to remove residual heat shall be provided. The system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified acceptable fuel design limits and the design conditions of the reactor coolant pressure boundary are not exceeded.*

Suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

Note that in this example, for the purposes of the CMS, the requirement would be typically parsed into three or four sub-requirements to make crafting the subsequent DBSs more effective. Parsing requirements appropriately will minimize confusion and make the SSC-Requirement relationships more visible.

Also note that Design Requirements are intentionally non-source specific. To include or exclude specific sources, craft an appropriate DBR.

DESIGN BASES SPECIFICATIONS

Design Bases Specifications are facility-specific. They restate Design Requirements into statements that specify what your unique facility will do to comply with a specific requirement. They are as made as specific as possible and still address how the requirement is met by the facility as whole, not by the system, component or structure.

Definition: *Design Bases Specifications are statements that define how your facility will comply with a specific Design Requirement.*

Example: *At the West Bend Nuclear Plant, residual heat will be removed under normal conditions by using the High Pressure Core Spray System when vessel pressure is above 700 psig, Low Pressure Core Spray when system pressure is 700 psig or below, and transferred through the Residual Heat Removal System to the Essential Service Water System and ultimately through the cooling towers to atmosphere.*

Under situations when off-site AC power is not available...

Suitable redundancy will be provided...

Note that general requirements can often produce very complex and convoluted DBSs necessary to specify the range of plant systems and configurations necessary to comply with the requirement. In the past, these complex conditional statements would be found in the Final Safety Analysis Report (FSAR) or similar document, but in the new CM taxonomy, these descriptions are placed to provide direct design guidance.

SSC SPECIFICATIONS

SSC Specifications translate the general plant-related DBS into specific functions and criteria for SSCs. SSC Specifications translate facility level DBS statements into the specific functions and specifications necessary for unique systems, components, or structures. In the NEI 97-04 taxonomy, these would be considered SSC Functions, but the term Specification was used here to reflect the broader sense of a system, structure, or component requirement.

Definition: *SSCS are statements that define how a particular SSC will fulfill a specific Design Bases Specification.*

Example: *The Residual Heat Removal System will transfer a minimum of 10 million btu/hr to the Essential Service Water System during normal cool-down operations.*

SUPPORTING DESIGN INFORMATION

Supporting Design Information (SDI) is historically what is considered ‘design bases’ information. It is the engineering information used to translate system, structure, or component related SSCs into physical systems, structures, or components. SDIs might be prepared by architect/engineers, component vendors or other sub-contractors. In the past, this design bases information was difficult to manage because source documentation was often not available. The new CM taxonomy accommodates this and the management of proprietary information by providing mechanisms to reflect critical calculation results and other numbers without necessarily requiring the supporting calculation or information.

Definition: *Supporting Design Information includes drawings, calculations, calculation results, and documents necessary for fulfilling a SSC Specification and procuring the associated SSC.*

Example: *WBNP Calculation Number 1-1985-206, Rev. 5, Minimum RHR Heat Load during Normal Cooldown Operations.*

SUPPORTING OPERATING INFORMATION

Supporting Operating Information (SOI) is a category provided in the taxonomy to accommodate information not necessary for the design, but required during operation or maintenance to ensure the design criteria are met. This might include items like lubrication schedules, or operator actions required during off-normal conditions.

Definition: *Supporting Operating Information is defined as Operating, Emergency, Maintenance, and Surveillance Procedures and other documentation necessary for the operation and maintenance of the facility to fulfill specific requirements.*

Example: *WBNP Normal Operating Procedure NOP-53-207, Rev. 32, Normal Cooldown Operations.*

DESIGN PARAMETERS

Design Parameters are typically inputs and outputs from calculations, or other specific values passed from a requirement, and include Design Limits, Operating Limits, alarm and trip setpoints, and Range of Normal Operation values for all systems and components.

Definition: *Design Parameters are defined as numbers with associated units that define characteristics, setpoints, and limits, associated with unique SSCs.*

Example: *Minimum Analyzed Design Limit RHR Heat Load during Normal Cooldown Operations: 10 million btu/hr*

Since Design Parameters represent calculation results that bound system and component performance, they facilitate Margin Management and Setpoint Management with little additional effort.

It is not the purpose of this document to discuss the ramifications or details of Margin Management or Setpoint Management, but to identify the ease by which Margin and Setpoint Management can be conducted with an effective CM taxonomy.

NEW CMS TAXONOMY EXAMPLE

A practical example of the new Configuration Management taxonomy is demonstrated in Figure 2. Here the relationships between the various examples used in the previous section can be observed.

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

Fig. 2– Practical Example of New Configuration Management Taxonomy

SUMMARY

The advantages of the new Configuration Management Taxonomy include:

- Assurance that the health and safety of the public is protected by design.
- Public and regulatory trust is enabled by demonstrating that the plant is operated as promised.
- Assures compliance with all Design Requirements.
- Captures the knowledge of an aging and retiring workforce.
- Avoids significant lost production from loss of trust or deviation from compliance.
- Provides a direct connection between systems, structures, and components and the associated requirements.
- Reduces substantially time and effort required to conduct engineering changes.
- Enables practical Margin Management and Setpoint Management

There are consequences to adapting the new Configuration Management Taxonomy.

- Software and necessary hardware is required to implement and manage the CM system.
- The Final Safety Analysis Report is no longer a source document for design bases information, but becomes an output report of the CM system.
- Artificially constructed Design Bases Documents are no longer necessary, again, they became output reports of the CM system.

In conclusion, the new Configuration Management Taxonomy enables management of all Design Requirements, complex requirement-to-component relationships, and design parameters, down to the individual system, structure, or component. It eliminates artificial constructions used in the past to manage design bases, and provides a mechanism for efficiently maintaining regulatory compliance documents. It eliminates unnecessary overhead in engineering design change and procurement improving economic viability. Finally, the new taxonomy is absolutely necessary for fulfilling the public promise of safe operation of nuclear production facilities in accordance with design.

REFERENCES AND FOOTNOTES

- [1] Taxonomy: a scheme of classifications
- [2] Zimmer, Cincinnati, Ohio, USA, 1984
- [3] INSTITUTE OF NUCLEAR POWER OPERATIONS, AP-929, *Configuration Management Process Description*, 2005
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA-TECDOC-1335, *Configuration Management in Nuclear Power Plants*, 2003
- [5] T. Winograd and F. Flores, *Understanding Computers and Cognition: A New Foundation for Design*, Addison-Wesley Publishing Company, 1987